ISOAG Meeting

August 2, 2017

Welcome to CESC

Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson

August 2, 2017

ISOAG August 2, 2017 Agenda

I. Welcome & Opening Remarks	Mike Watson, VITA
II. Investigations, Law Enforcement and the Cloud	Steven Hernandez, HHS,OIG
III. Enterprise Cloud Oversight Services	Demetrias Rodgers, VITA
IV. Building a Pentest Program on a Shoestring Budget	Grayson Walters, TAX & Andy Hallberg, ABC
V. Upcoming Events	Mike Watson, VITA
VI. Partnership Update	Northrop Grumman

Information Assurance Overview: Cloud, Trusted Internet Connections and Continuous Monitoring

Steven Hernandez
Chief Information Security Officer
HHS/OIG

August 2nd 2017

Agenda

- Introduction
- Cloud assurance overview
- Cloud Assessment
- Continuous Monitoring Challenges in the Cloud
- Trusted Internet Challenges in the Cloud
- Legal concerns with cloud providers
- Litigation Hold and eDiscovery
- Moving forward with best recommendations
- Questions

Introduction

- Who I am:
- **Steven Hernandez** MBA, CISSP, CISA, CSSLP, CAP, SSCP, CNSS(4011-4016), HCISPP, ITIL
  - Director of the HHS/OIG Information Assurance Division
  - Chief Information Security Officer

What is Cloud?

- Possibilities:
  - Software as a Service (SaaS)
    - Vendor is responsible for the vast majority of security control implementation and operation.
  - Platform as a Service (PaaS)
    - Vendor is responsible for typically the operating system and hardware security controls.
  - Infrastructure as a Service (IaaS)
    - Customer is responsible for the Majority of Controls.

Security Control Responsibility

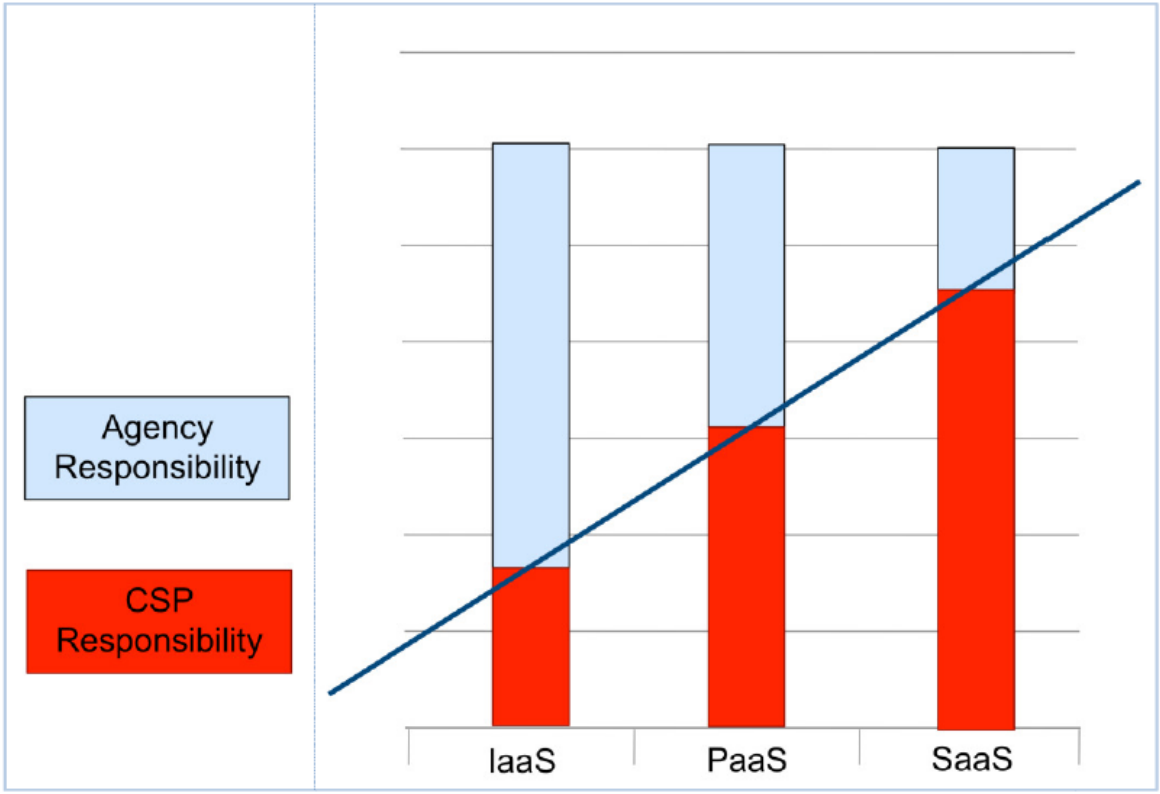
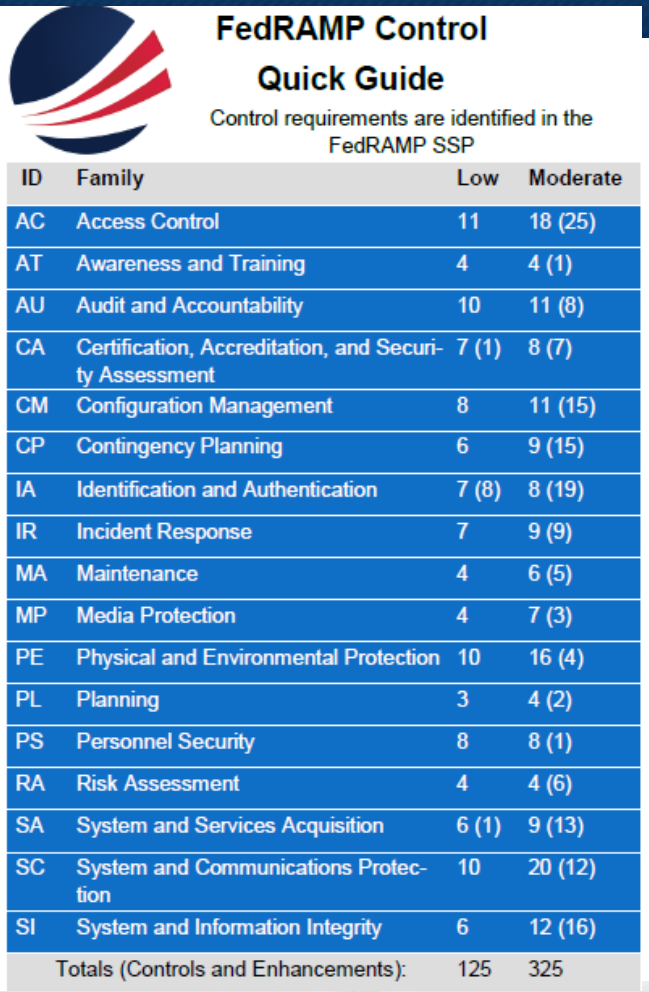


Figure 7-2. Security Control Responsibilities

Security Controls: Low and Moderate



FedRAMP Control Quick Guide

Control requirements are identified in the FedRAMP SSP

ID	Family	Low	Moderate
AC	Access Control	11	18 (25)
AT	Awareness and Training	4	4 (1)
AU	Audit and Accountability	10	11 (8)
CA	Certification, Accreditation, and Security Assessment	7 (1)	8 (7)
CM	Configuration Management	8	11 (15)
CP	Contingency Planning	6	9 (15)
IA	Identification and Authentication	7 (8)	8 (19)
IR	Incident Response	7	9 (9)
MA	Maintenance	4	6 (5)
MP	Media Protection	4	7 (3)
PE	Physical and Environmental Protection	10	16 (4)
PL	Planning	3	4 (2)
PS	Personnel Security	8	8 (1)
RA	Risk Assessment	4	4 (6)
SA	System and Services Acquisition	6 (1)	9 (13)
SC	System and Communications Protection	10	20 (12)
SI	System and Information Integrity	6	12 (16)
	Totals (Controls and Enhancements):	125	325

Cloud Control Req.

- FedRAMP High Impact Control Baseline
  - Finalized June 22nd 2016
  - Implements the NIST SP 800-53 Rev 4 “High” baseline controls
  - Would allow CSP’s to handle most all data with the exception of classified data and data subject to specific legal requirements
  - Approx. 421 Control Test Points

Cloud Control Req.

- FedRAMP High Impact Control Baseline
  - Why? Only 20% of federal systems need this?
  - Because 50% of federal spending is on High impact systems!
  - Three Vendors are Piloting
    - CSRA/Autonomic Resources – ARC-P PaaS
    - Microsoft – Azure Government
    - Amazon Web Service – AWS GovCloud

Federal Agency Responsibilities 12/08/11

https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf

d. Each Executive department or agency shall:

i. Use FedRAMP when conducting risk assessments, security authorizations, and granting ATOs for all Executive department or agency use of cloud services;

ii. Use the FedRAMP PMO process and the JAB-approved FedRAMP security authorization requirements as a baseline when initiating, reviewing, granting and revoking security authorizations for cloud services;[10]

iii. Ensure applicable contracts appropriately require CSPs to comply with FedRAMP security authorization requirements;

iv. Establish and implement an incident response and mitigation capability for security and privacy incidents for cloud services in accordance with DHS guidance;

v. Ensure that acquisition requirements address maintaining FedRAMP security authorization requirements and that relevant contract provisions related to contractor reviews and inspections are included for CSPs;

Federal Agency Responsibilities

https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf

vi. Consistent with DHS guidance, require that CSPs route their traffic such that the service meets the requirements of the Trusted Internet Connection (TIC) program; and

vii. Provide to the Federal Chief Information Officer (CIO) annually on April 30, a certification in writing from the Executive department or agency CIO and Chief Financial Officer, a listing of all cloud services that an agency determines cannot meet the FedRAMP security authorization requirements with appropriate rationale and proposed resolutions.

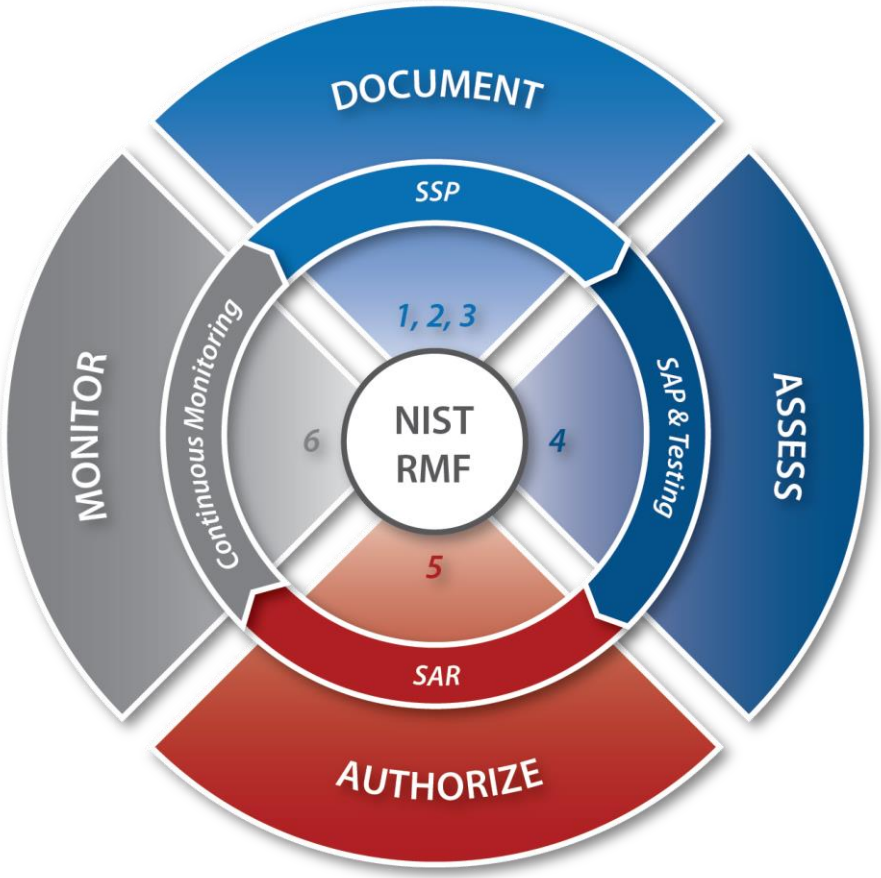
[10] For all currently implemented cloud services or those services currently in the acquisition process prior to FedRAMP being declared operational, security authorizations must meet the FedRAMP security authorization requirement within 2 years of FedRAMP being declared operational.

FedRAMP launched June 6th 2012: Agencies must be compliant since June 6th, 2014

Document Examples

- Templates (Fedramp)
  - https://www.fedramp.gov/
    - Package Request Form
    - Security Assessment Framework
    - Guide to Understanding FedRAMP
    - FedRAMP Revision 4 Transition Guide
    - Quick Guide to FedRAMP Readiness Process
    - FedRAMP Policy Memo
    - Security Controls
    - Control Quick Guide
    - Standard Contract Clauses
    - Control Specific Contract Clauses
    - Cloud Procurement Best Practices
    - Template FedRAMP ATO Letter
    - JAB Charter
    - Continuous Monitoring Strategy Guide
    - Significant Change Form
    - Incident Communications Procedure
    - Branding Guidance

Assessment Process



- The FedRAMP Agency ATO authorization process should follow the FedRAMP Security Assessment Framework (SAF)
- The FedRAMP SAF is based on the NIST Risk Management Framework (RMF)
- The FedRAMP SAF is available on FedRAMP.gov by navigating to the Resources -> Program Documents webpage

Document Check List – FedRAMP Templates

- FedRAMP templates are available at FedRAMP.gov on the Resources -> Templates webpage
- Agency ATO packages submitted to FedRAMP must include 14 FedRAMP templates
- The PMO will check these templates for completeness, critical security control showstoppers, and quality
- It's recommended that you use the Rev 4 Security Assessment Test Cases that the FedRAMP PMO released in Excel format for public comment: https://www.fedramp.gov/files/2015/01/FedRAMP-Security-Assessment-Test-Cases-Rev-4-v1 .xlsx

FedRAMP Templates Available:

- System Security Plan (SSP)
  - FIPS Pub 199
  - E-Authentication
  - Control Implementation Summary (CIS)
  - CIS Worksheet
  - IT Contingency Plan (CP) and CP Test
  - Privacy Threshold Analysis (PTA) / Privacy Impact Assessment (PIA)
  - Rules of Behavior (ROB)
- Security Assessment Plan (SAP)
  - Security Assessment Test Cases
- Security Assessment Report (SAR)
  - Security Test Cases
- Plan of Action and Milestone (POA&M)
- Agency ATO Letter

Submission of Cloud to GSA

1. CSP contracts with an accredited 3PAO and submits a 3PAO Designation Form to the FedRAMP PMO.
2. FedRAMP ISSO holds a meeting with CSP and 3PAO to discuss expectations and set timeframes for deliverables.
3. 3PAO creates and the FedRAMP ISSO approves a testing plan that ensures the assessment will cover the state authorization boundary and controls.
4. 3PAO performs and independently tests the CSP's system and generates a Security Assessment Report (SAR) that documents findings and provides and analysis of the test results to determine the risk exposure.
5. CSP develops a Plan of Action & Milestones (POA&M) that addresses the specific tasks, resources, and schedule for correcting each of the weaknesses and residual risks identified.
6. CSP submits the SAR and POA&M to the FedRAMP ISSO for a completeness and overall risk posture review.
7. The Joint Authorization Board (JAB) makes a risk-based decision on whether to accept the vulnerabilities and planned fixes.
8. If JAB determines the risk level is too high it recommends remediation steps that the FedRAMP ISSO shares with the CSP.
9. CSP corrects control implementations, retests affected controls, and resubmits revised documentation
10. If JAB accepts the risks associated with the system, the FedRAMP ISSO notifies the CSP that they are ready to finalize the security assessment.

Is FedRAMP working?

- Yes!
  - Cloud providers are beginning to understand this is the minimum necessary to compete in the federal space. 82% of all cloud procurements are including FedRAMP requirements.
  - 73 CSPs have been deemed compliant (+28)
  - 4 CSPs in process for JAB PATO (-6)
  - 40 CSPs in process for Agency ATO (+12)
  - 3 CSPs are FedRAMP “ready”
  - Marketplace.fedramp.gov

Continuous Monitoring

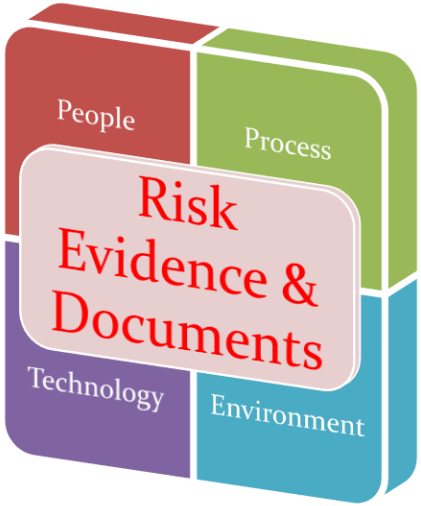
- Continuous Monitoring has always been part of the NIST Risk Management Framework (RMF!)
- Continuous monitoring has always been part of the certification and accreditation/authorization process.
- Why does Certification/Assessment and Authorization matter?
  - Understanding the risk you take when using a system
  - Understanding the limitations and strengths of a system
  - Having a level of assurance and due diligence for a system
  - Continuously monitor a system for vulnerabilities and resulting risk
  - It's the Law! FISMA requires we do this and for good reason!

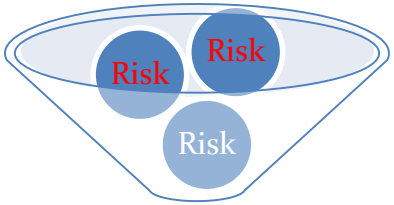
Overall Risk View

Rolling up comprehensive risk information for sound decision making!

Continuous Monitoring
Automated Process Areas
DHS/CDM

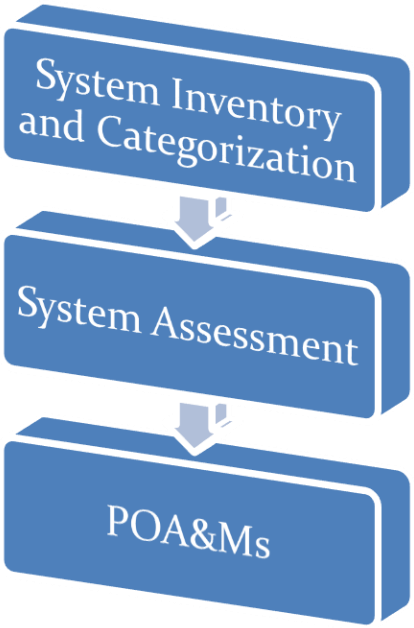
SAR





Decision

SAR



Manual Assessment
Process Areas
800-53A and Test Cases

Cloud Continuous Monitoring

- When the vendor controls everything how can we ensure risk visibility?
- Remember:
  - FedRAMP is going to ensure the CM capability exists for the cloud provider in three areas:
    - Operational Visibility
    - Change Management
    - Incidence Response

Cloud Continuous Monitoring

Cloud Continuous Monitoring

- Operational Visibility:
  - Operational visibility provides a look-in into the security control implementations of the CSP
    - What contract language or clauses does the organization have for ongoing and as needed (ad hoc) security assessments?
    - How much visibility through automated or manual assessments does the organization have into the cloud provider.
- Change Control and Management:
  - How does the cloud provider control changes and configurations? What assurance does the organization and agency have that breaches or downtime will not occur due to unintended changes or poorly tested changes?

Cloud Continuous Monitoring

- Incident Response and Law Enforcement
  - What automated scanning, patching and reporting is available to the agency?
  - Is the cloud provider using SCAP compliant tools and providing DHS compliant feeds back to the agency?
  - What contractual provisions are in place for internal investigations, employee monitoring and formal investigations?

Cloud Continuous Monitoring

- Recommendations:
  - Ensure contractual provisions exist which ensure the cloud provider must provide SCAP compliant configuration, asset, vulnerability and patch status for DHS CDM dashboards and feeds.
  - Ensure contracts are vetted by law enforcement partners and Legal to ensure all legal actions are routed to the appropriate agency resources and when the agency needs information from the cloud provider there are no surprises.
  - Ensure you have the ability to send in an independent assessment team to perform ad hoc or after action assessments.
  - Ensure a full FedRAMP provisional ATO (or FedRAMP Ready) is required for new contracts and re-competing existing contracts which do not contain the FedRAMP requirements.

Audit and Inspection Clauses

- A critical item for Agencies and IGs
  - FedRAMP does NOT cover access for investigations and audits and reviews
    - Legal Route:
      - Time consuming, expensive, confrontational
    - Contractual Route is much better!
      - Include specific terms related to access to facilities, data and metadata
      - "Yellow-Book" auditing standards
        - » In addition to FedRAMP Controls
        - » Agencies should demand Yellow-Book standards starting with the High Baseline and working back to Moderate
        - » Several CIGIE working groups are working through this but we need to be unified in our approach!

Audit and Inspection Clauses

- Dept of Ed OIG

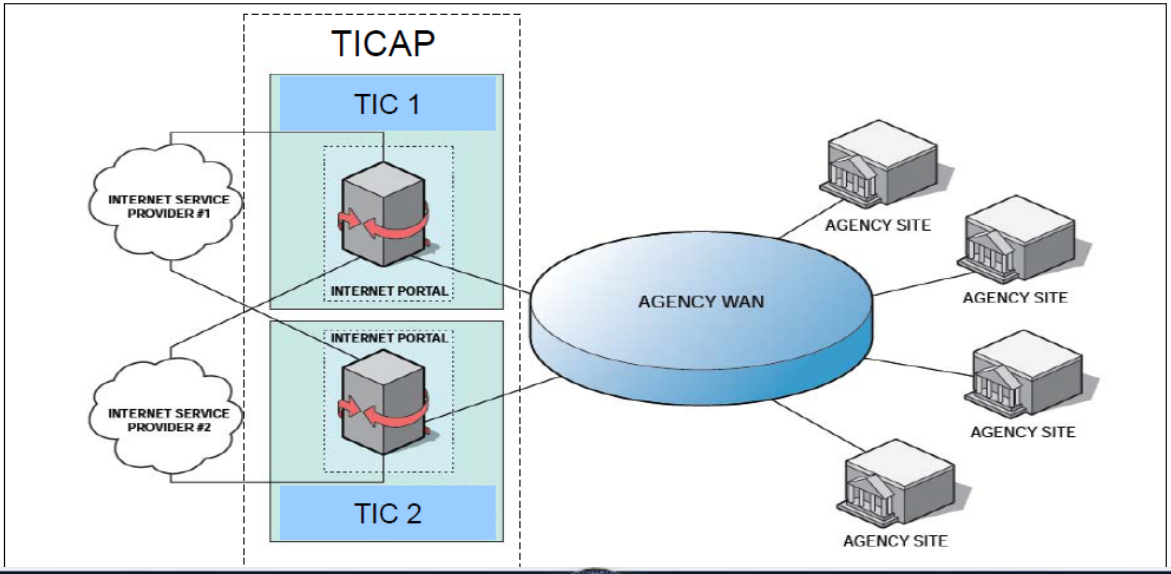
- Class Deviation to Implement Policy Regarding Access to Contractor Information Systems

- The purpose of this alert is to issue a class deviation that allows Contracting Officers to require contractors and subcontractors at all tiers to afford the Department, other Federal agencies, the Comptroller General of the United States, and their authorized third-party representatives, full and timely access to contractor information systems and related resources to perform privacy and information security inspections.

Trusted Internet Connections

TIC Glossary

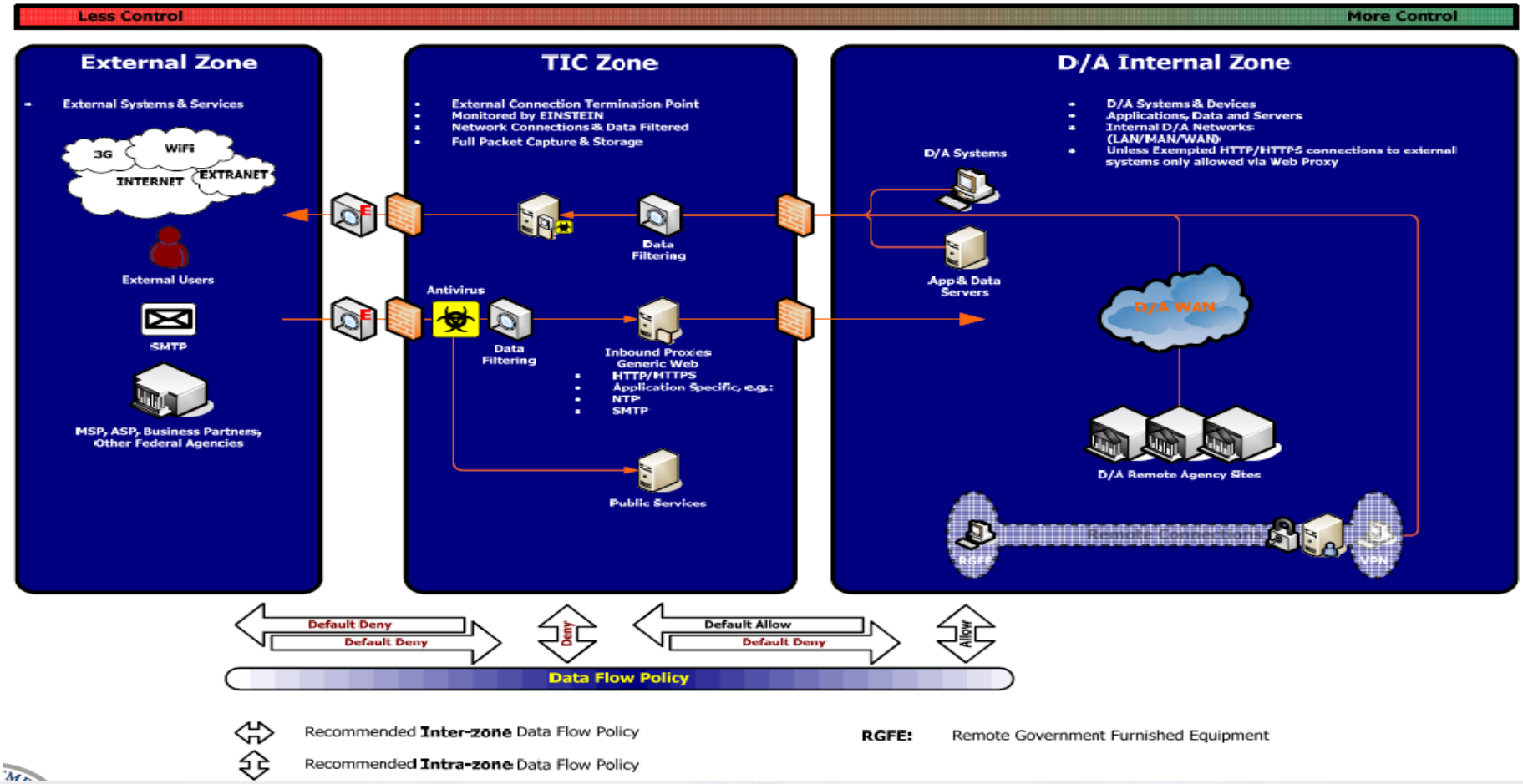
- **TIC**: Facility. Physical location containing security hardware & software
- **TICAP**: Access provider that manages the operation of TICs in support of customer requirements and policies; includes two or more TICs, two or more connections as well as the supporting NOC/SOC functions
- **MTIPS**: Service sold by a Networx vendor, also a TICAP



Trusted Internet Connections Required through:

- Presidential Directive: HSPD 23, Comprehensive National Cybersecurity Initiative (Initiative #1 is Trusted Internet Connections Initiative)
- TIC Working Group: agency-designated technical experts have participated in several work group sessions to develop TIC technical requirements, clarify architecture, and resolve technical question
- CIO Council: agency CIOs have been briefed on several occasions both on the status and expectations of TIC requirements.
- Government wide meetings: Held in Q1 & Q2FY08, used to outline the expectations of the TIC Initiative, communicate notional architecture, and answer agency questions
- OMB publication of Memo 08-16, Guidance for the TIC Statement of Capability
- "Continue to pursue the goal of the Trusted Internet Connection program to reduce the number of government network connections to the Internet but reconsider goals and timelines based on a realistic assessment of the challenges." – Cyberspace Policy Review, The White House, 2009

Trusted Internet Connections:



What about Cloud and Trusted Internet Connections?

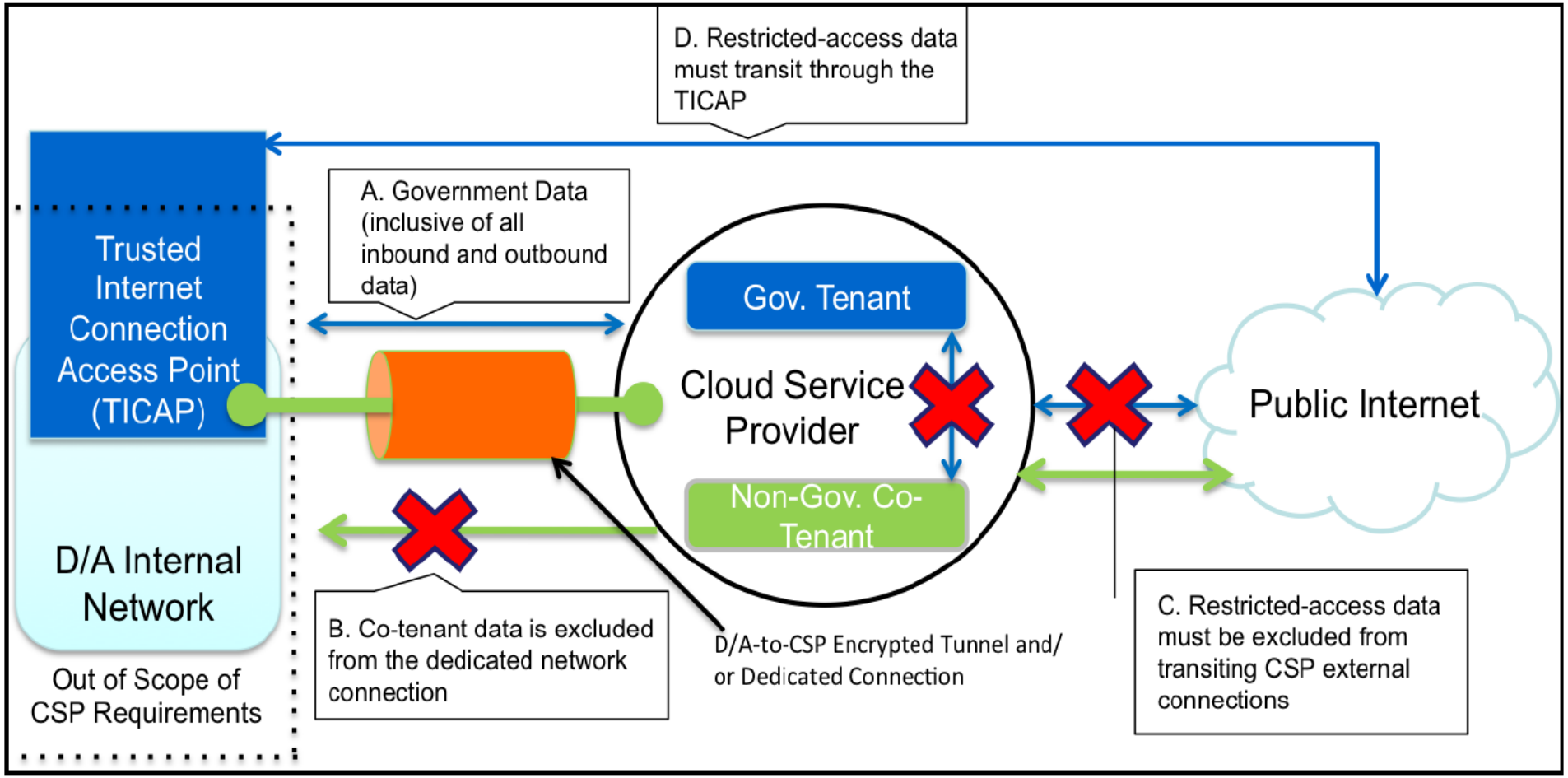
Three Defined Use Cases for Connecting to CSPs

- Public Unrestricted Data (e.g. public website)
  - TIC is not Needed
- System for internal Agency use (e.g. internal CRM tool)
  - Connection to CSP must use dedicated connection
- System with mixed use that has restricted data for both internal and external users (e.g. email)
  - TIC applies

Three Architectural Options for Routing Traffic to External Parties through a TIC

1. Agency places an MTIPS connection at the CSP's data center(s)
2. Route all traffic from CSP to Agency through a VPN, WAN or other dedicated network connection, external traffic passes through Agency TIC
3. Proxy traffic from CSP to Agency TIC when bound for external traffic (traffic destined to Agency must still be tunneled or encrypted)

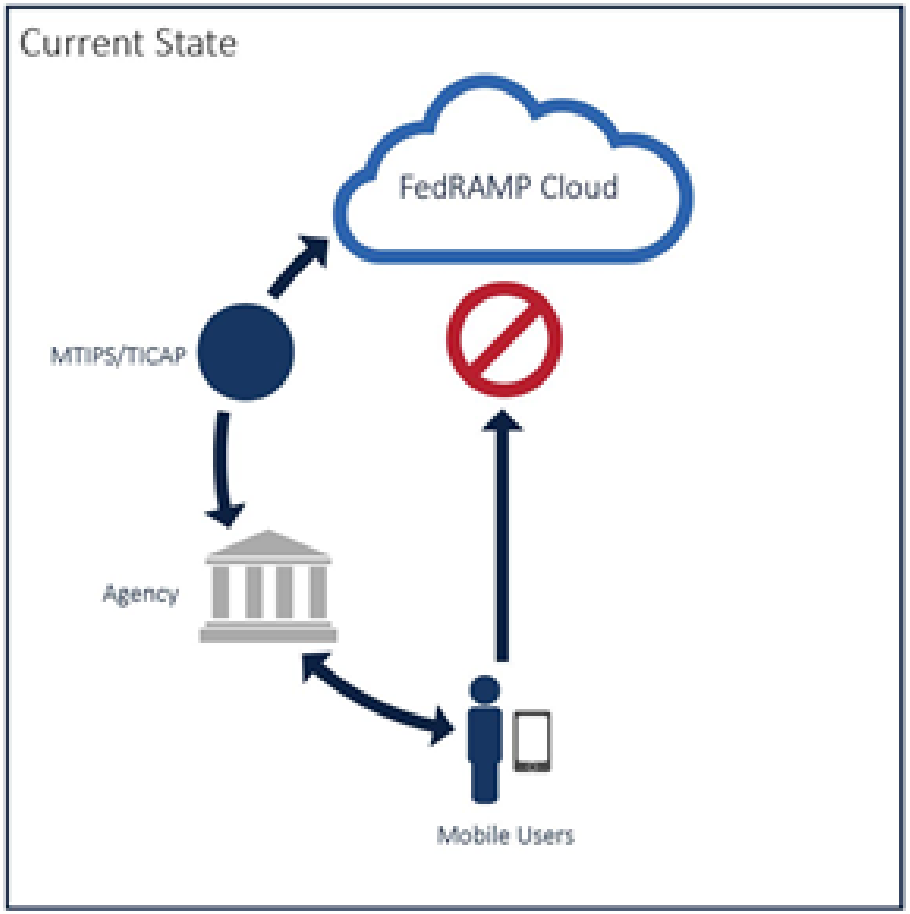
Trusted Internet Connections

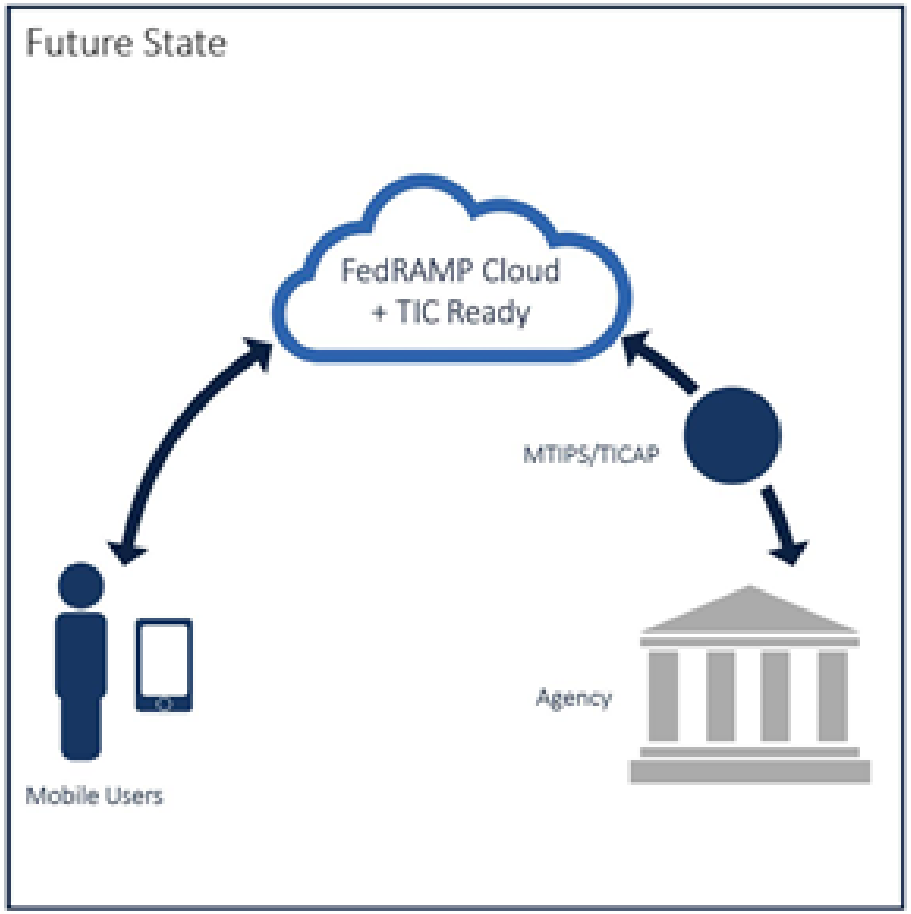


What have we learned from vendors?

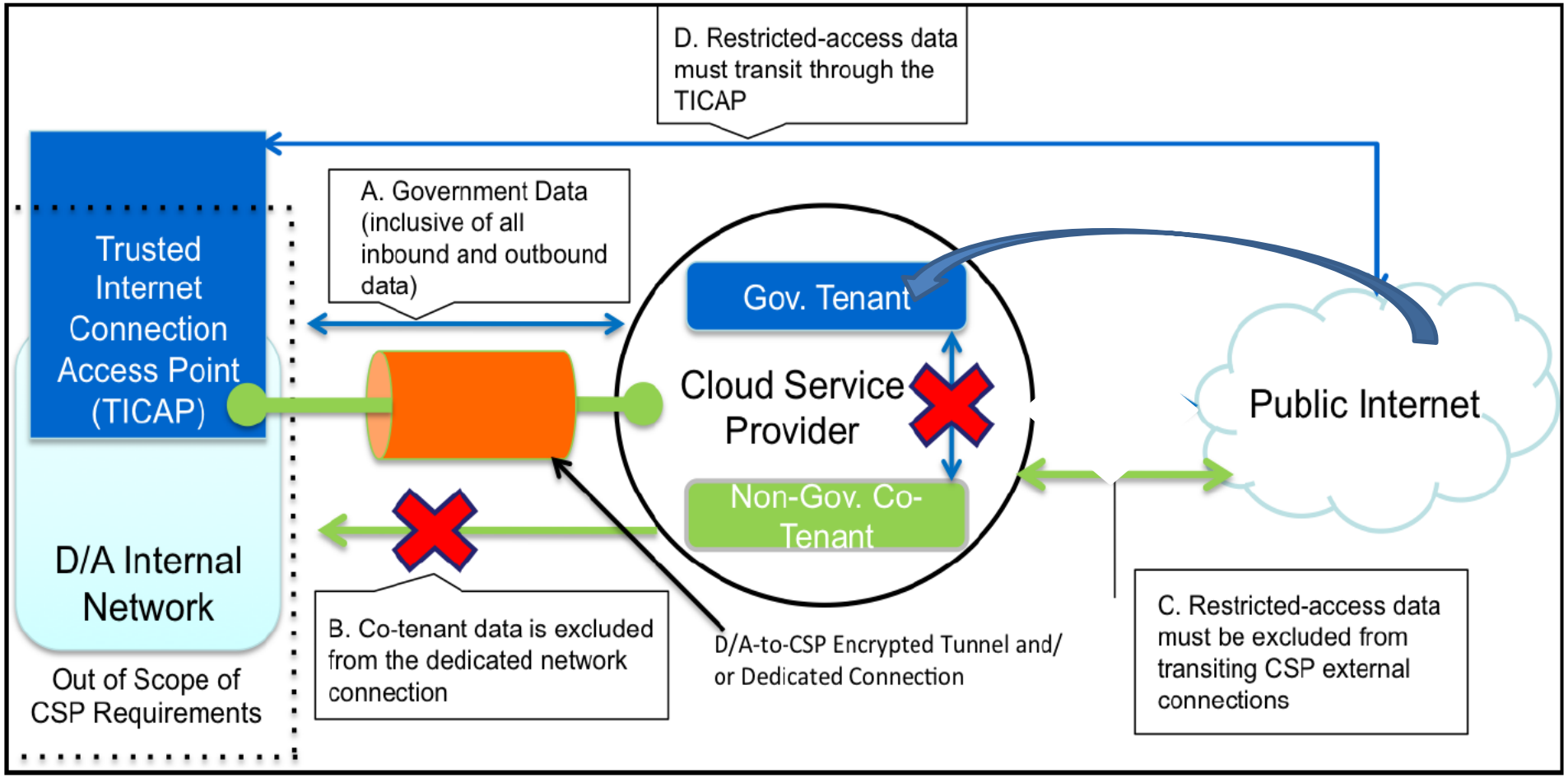
- FedRAMP does not enforce TIC
  - SC(7)-1 is a hybrid responsibility control
  - FedRAMP ensures CSP has architecture exists to support TIC – separation of data, clear boundaries, etc.
  - Agency must ensure that they route traffic to meet TIC requirements
- Vendors are unhappy with current approved architectures
- Inhibits true value of cloud
- Many agencies do not enforce

Future Resolution
(CSP TIC Overlay?)





Future Resolution
(CSP TIC Overlay?)



Future Resolution
(CSP TIC Overlay?)

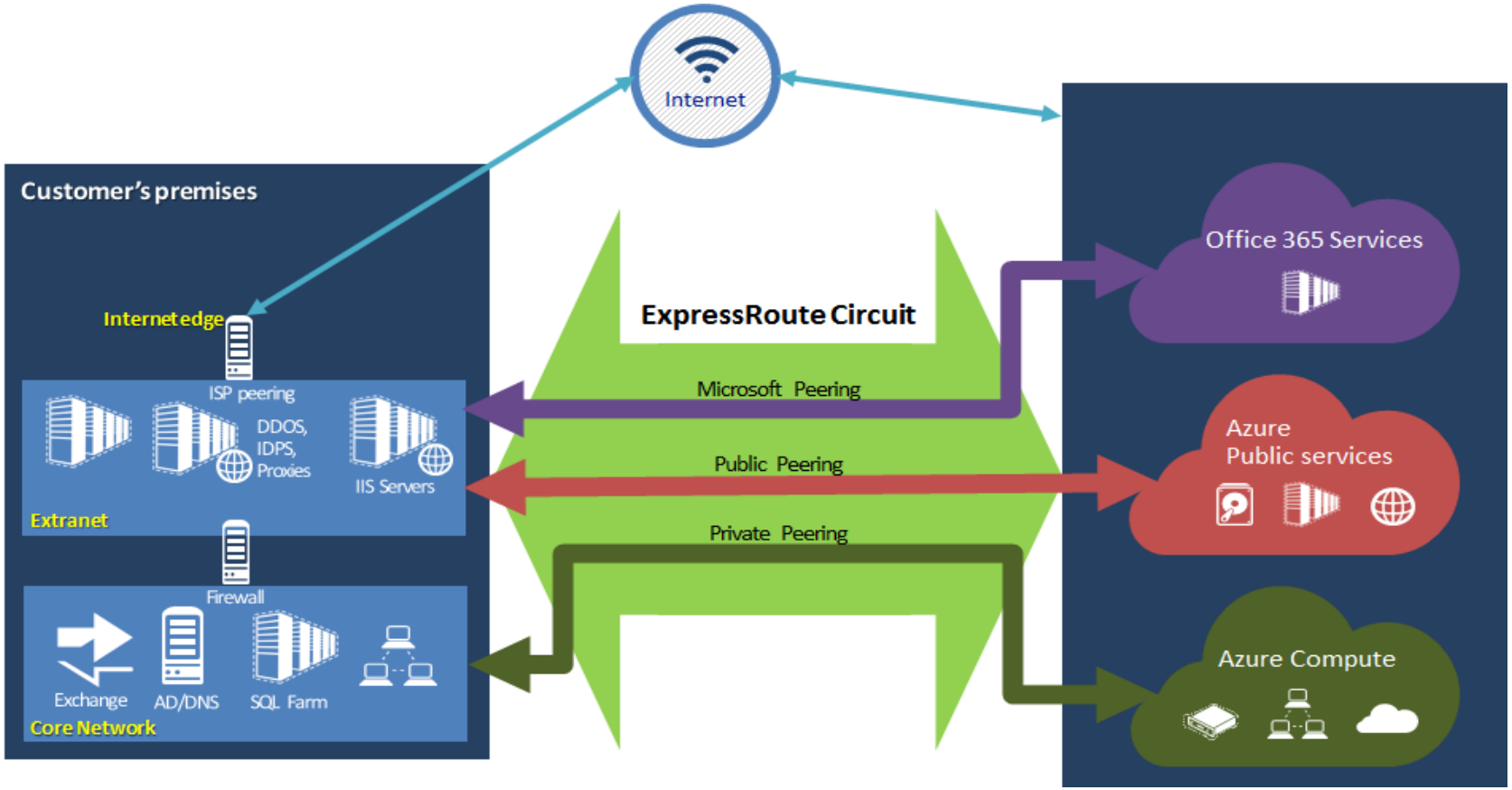
- Not all TIC capabilities are represented in the FedRAMP-TIC overlay as not all TIC capabilities are applicable to CSPs.
- The TIC capabilities and the FedRAMP security control requirements are not a one-to-one mapping; some are one-to-many, many-to-one, or many-to-many.
- The TIC Reference Architecture v2.0 defines TIC capabilities as either Recommended or Critical. For purposes of this overlay, ALL applicable TIC capabilities are considered Critical (and therefore mandatory) for external cloud service providers.
- Achieve a FedRAMP security authorization by an authorizing official (agency or JAB) based on the 3PAO Security Assessment Report; and
- Be deemed "TIC Ready" by DHS based on DHS's review of a 3PAO TIC Capabilities Assessment Report
- AWS Amazon completed a pilot in Feb of 2016. Results indicate a substantial amount of collaboration is necessary between agencies, providers and DHS to be successful. (https://do.awsstatic.com/whitepapers/compliance/Guidance_for_Trusted_Internet_Connection_TIC_Readiness_on_AWS.pdf)

Future Resolution
(CSP TIC Overlay?)

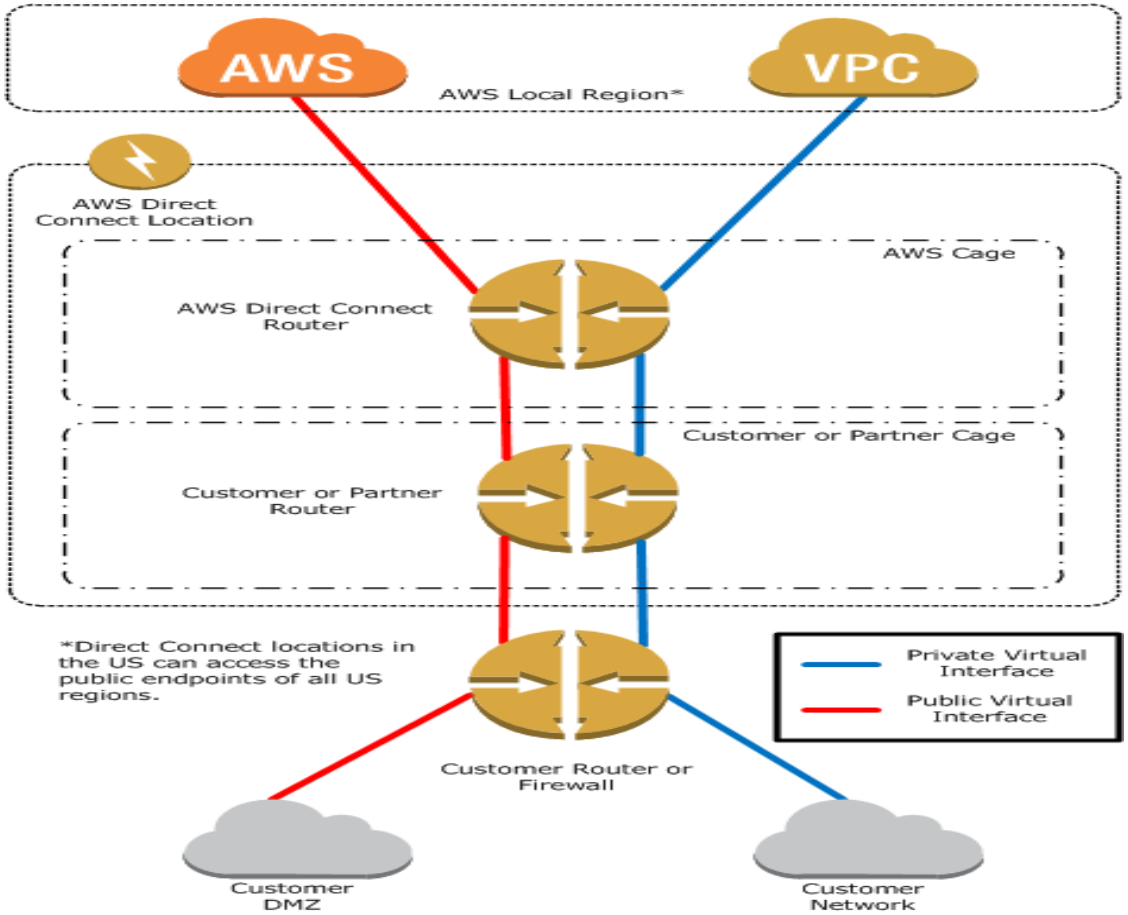
- Outlook:
  - Uncertain if CSP can meet equivalent requirements of MTIPS
  - Questions as to the level of integration with US-CERT and Agency monitoring capabilities
  - Costs are still uncertain as the CSP may have to significantly re-engineer their networking to accommodate this model.

- If successful could mean more providers of MTIPS services
  - Drive down costs
  - Increase competition
  - Increase performance

Future Resolution
(Direct Connect, ExpressRoute etc.)



Future Resolution
(Direct Connect, ExpressRoute etc.)



Legal Hold, Records Retention, FOIA, eDiscovery and all this fun!

Sounds complex and our lawyer friends make a solid living around these terms:

Basically two functions:

1. Can you preserve information based on a criteria and a timeline?
2. Can you search your collections in a forensically sound manner?

Litigation Hold Example (O365)

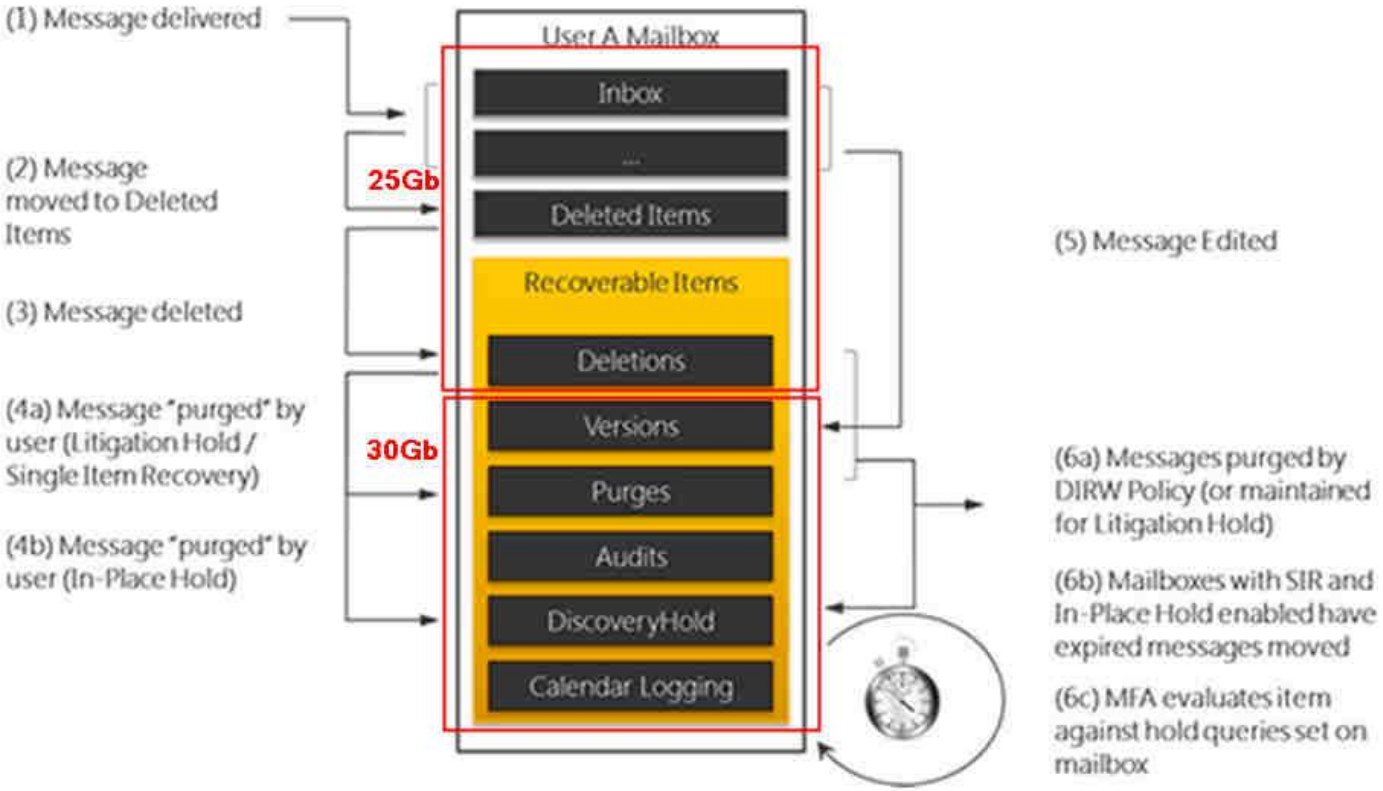


Figure 5: Deleted items and original copies of modified items are preserved in the Recoverable Items folder of each mailbox

Example (O365)

Hey Bob, Didn't we tell the lawyers we can only store 6 months worth of email?

You're living way in the past! With our new cloud provider our legal hold is indefinat..... Uhh ohh....

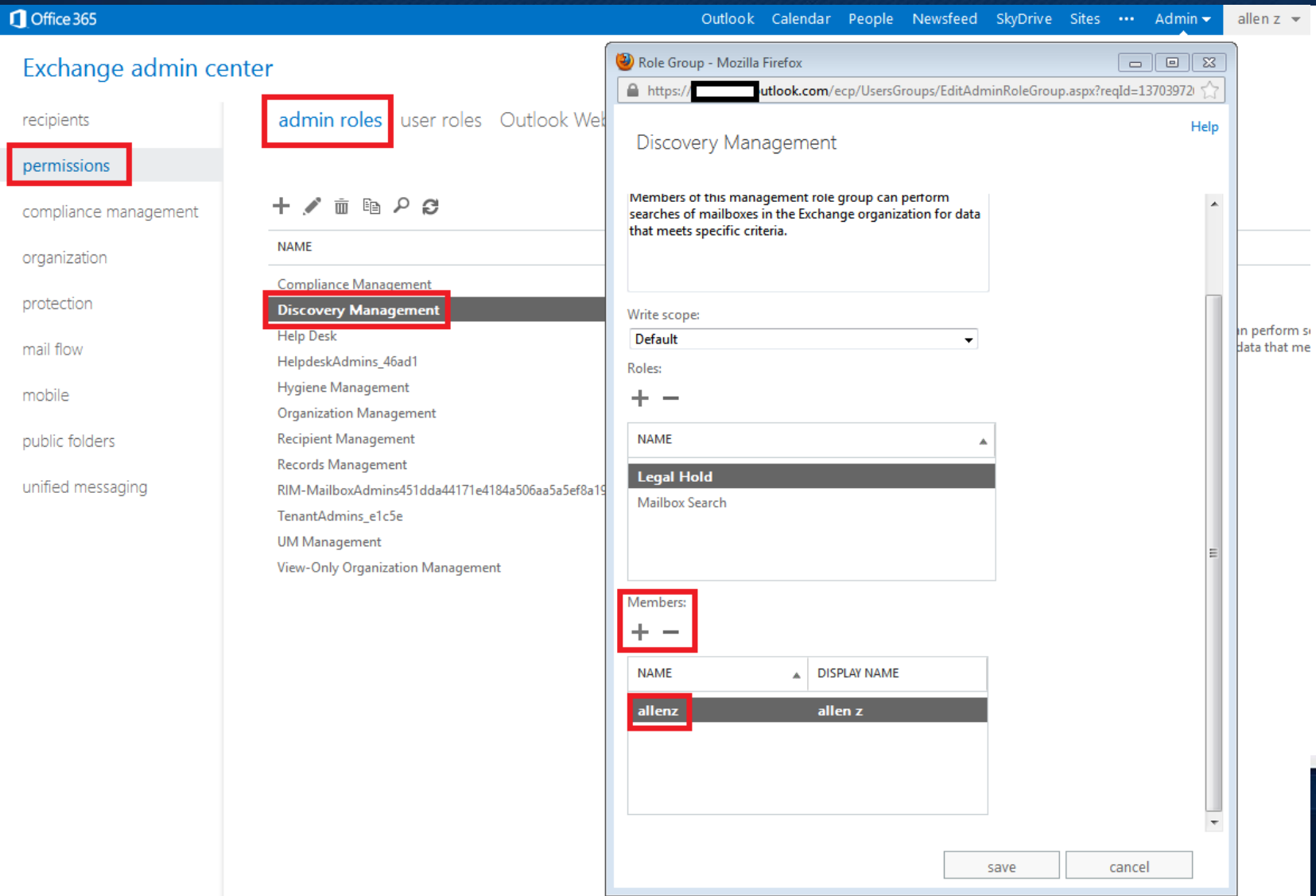
1. In-Place Hold

In-place hold: content stays in Exchange and SharePoint, less storage space, lower costs, higher fidelity

Location and query based: hold entire mailboxes, SharePoint sites, or apply a query to hold less content

No impact to users: seamlessly create, edit, and delete without knowing its on hold

E-Discovery Example (O365)



E-Discovery

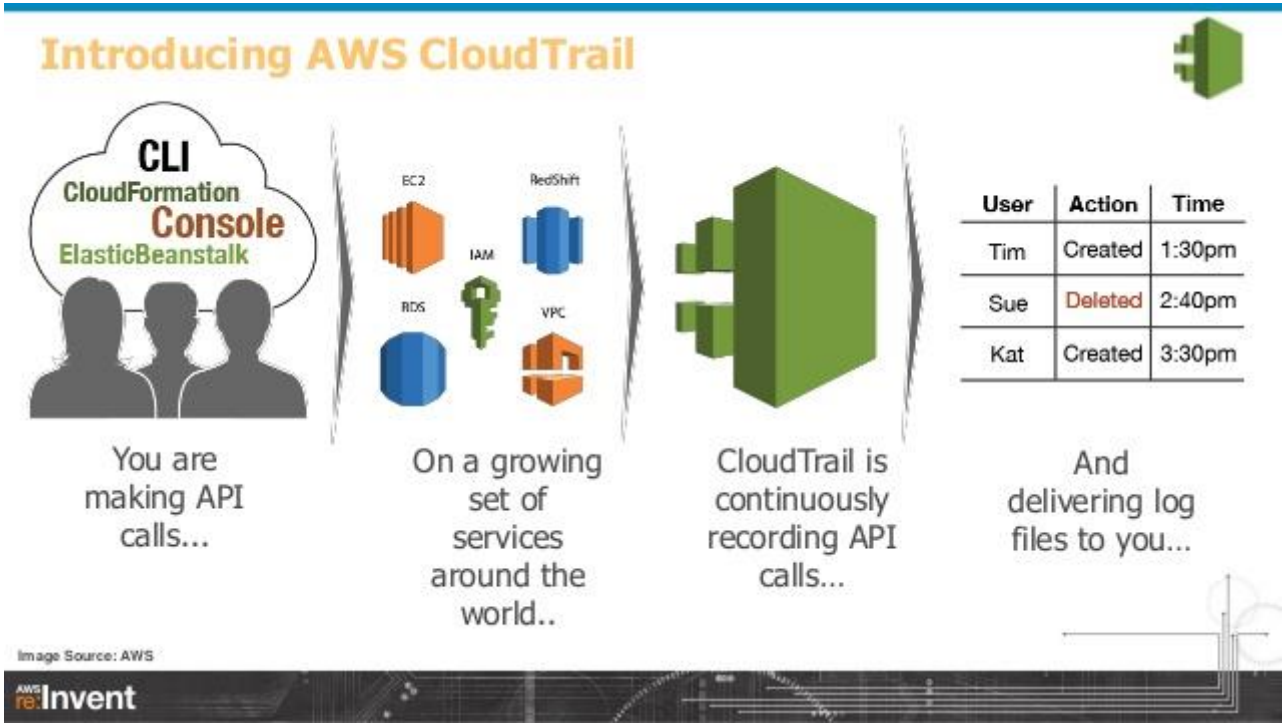
Remember:

- Separation of duties
  - E-Discovery is a powerful tool
    - Admins snooping
    - Mangers going on fishing trips
  - Contract up-front for capability
    - Storage
    - Tools
    - Capabilities
    - SaaS most likely

Forensic Examples

The Good:

- Logging: AWS Cloudtrail



Forensic Examples

The Good:

- Least Privilege: Microsoft Lockbox

Critical concerns contracting officers:

Pity the CO (at least at DoD for now…):

Appropriate requirements to support applicable inspection, audit, investigation, or other similar authorized activities specific to the relevant types of Government data and Government-related data, or specific to the type of cloud computing services being acquired;

Appropriate requirements to support and cooperate with applicable system-wide search and access capabilities for inspections, audits, investigations, litigation, eDiscovery, records management associated with the agency's retention schedules, and similar authorized activities; and……

WE CAN HELP!

Questions

Thanks!!

Contact Me:

Steven Hernandez

Steven.hernandez@oig.hhs.gov

Virginia Information Technologies Agency

Enterprise Cloud Oversight: The What and When

Demetrias Rodgers
Enterprise Services Director

ISOAG
AUG 02, 2017

ECOS – The What

- Enterprise cloud oversight service
  - Standardized service-based approach to security assessment, authorization and ongoing monitoring for cloud based services consumption
- Framework widely used across various levels of government as published in NIST 800-37
  - FedRamp simplified NIST Risk Management Framework by creating four process that encompass the six steps within 800-37
    - Document
    - Assess
    - Authorize
    - Monitor

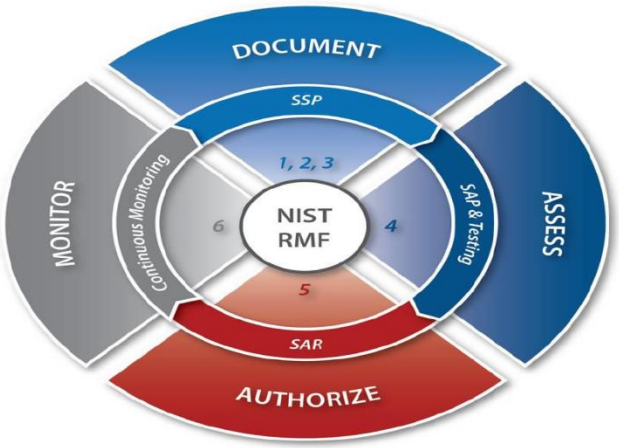
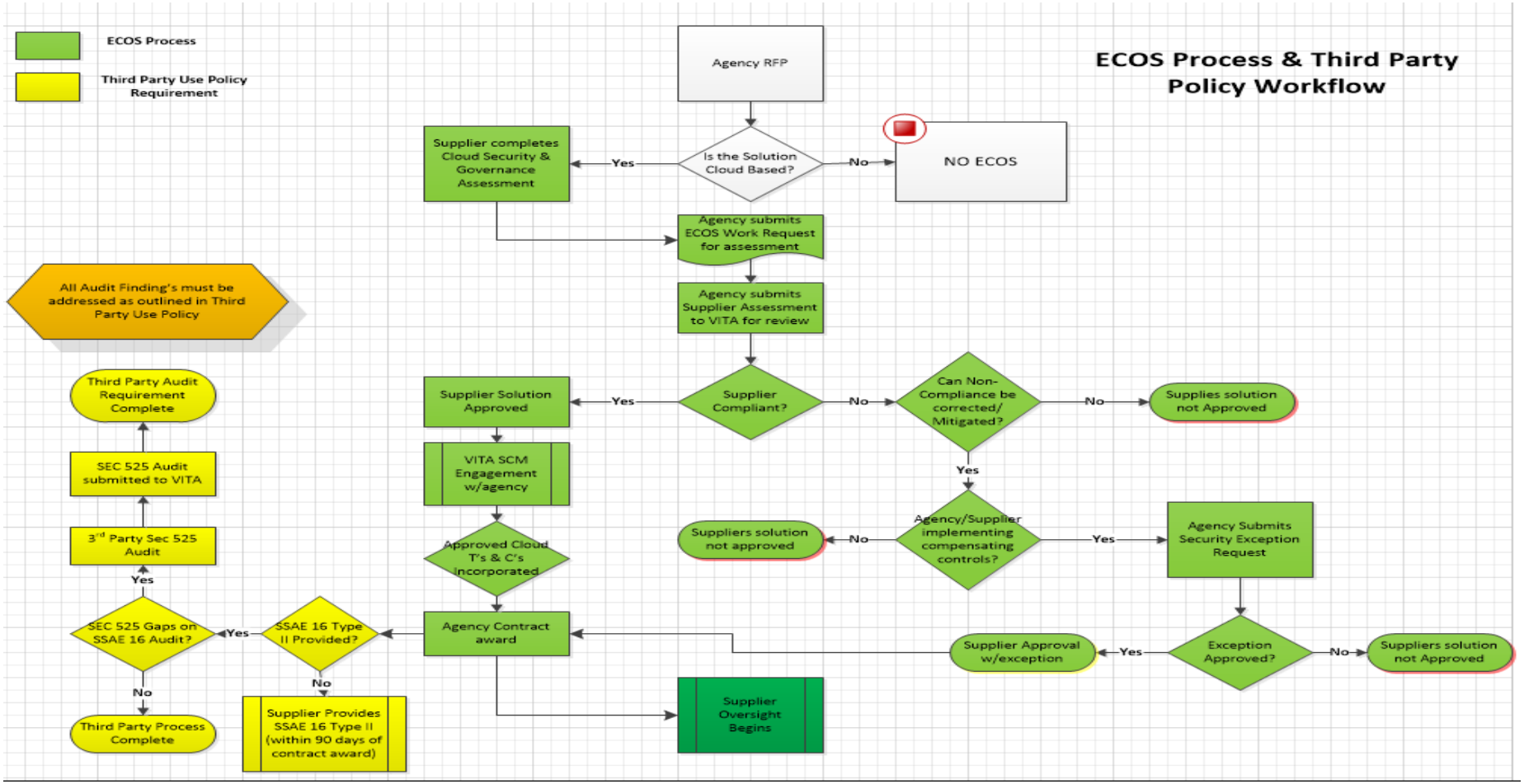


Figure 3-1 – FedRAMP Risk Management Framework

ECOS – Security Assessment

- Lack of transparency into cloud providers security posture is and remains a primary inhibitor to cloud adoption.
- The Cloud Security Assessment
  - VITA's assessment questionnaire consists of (currently)121 questions covering various control groups.
  - The format is largely based the Cloud Security Alliance's Consensus Assessments Initiative Questionnaire
  - Assists the suppliers in understanding the security requirements of the commonwealth as well as allows for agencies to understand areas of concern.

ECOS – The What (Process and Policy)



ECOS – For Which Cloud Services

- ECOS is a service **specifically** created for third-party suppliers offering SaaS applications
- **What is SaaS?**
  - Capability provided to the consumer is to use the provider's applications running on a cloud infrastructure
  - Applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.
  - Consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user specific application configuration settings

ECOS – For Which Cloud Services

- **SaaS characteristics**
  - Network-based access to and management of commercially available software
  - Supplier-provided services accessed through an internet connection to a third-party hosted facility
  - Service delivery typically a one-to-many model (single instance, multi-tenant architecture); generally includes common architecture for all tenants, usage based pricing and scalable management
  - Third party supplies management of the service, including functions such as patching, upgrades, platform management, etc.
  - Multi-tenant architecture, all users and applications share a single, common infrastructure and code base that is centrally maintained
  - Subscriber/user manages access controls for the application
  - Provider is *data custodian and server administrator*

ECOS – The When

- **ECOS applies**
  - Services being procured meet the above definition and/or characteristics of a software as a service (SaaS) provider
  - ECOS does not cover PaaS requests as part of the current service. PaaS solutions are available through the eGov contracts or through a hosting exception request.
  - When an agency is requesting the provider act on behalf of a Commonwealth entity and/or is accepting commonwealth data, serving as the *data custodian and/or system administrator* of that data for purposes of making it available back to the Commonwealth via an interface for fee.

Questions

Contact: Demetrias Rodgers
Demetrias.Rodgers@vita.virginia.gov

Backup Slides

Backup Slides

Platform as a Service Definition

- **What is PaaS?**
  - Capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider
  - The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
  - Services to develop, test, deploy, host and maintain applications in the same integrated development environment; varying services needed to fulfill the application development process
  - Web-based user interface creation tools help to create, modify, test and deploy different user interface scenarios

PaaS Use Cases & Characteristics

- **PaaS characteristics**
  - Services to develop, test, deploy, host and maintain applications in the same integrated development environment.
  - All the varying services needed to fulfil the application development process
  - Web based user interface creation tools help to create, modify, test and deploy different UI scenarios
  - Multi-tenant architecture where multiple concurrent users utilize the same development application
  - Built in scalability of deployed software including load balancing and failover
  - Integration with web services and databases via common standards
  - Support for development team collaboration – some PaaS solutions include project planning and communication tools
  - Tools to handle billing and subscription management

PENTEST ON A BUDGET

Presented @

Aug 2017 ISOAG

Grayson Walters ISO @ Tax

Andy Hallberg ISO @ ABC

You can just go hack yourself!

Level setting expectations

A compilation of two talks

- What this talk isn't
- What this talk is
- What you should take away
- How this will help in your day job

What are you trying to accomplish?

PENTEST

- Specific goal
  - Get a copy of the customer database
- Find a way to meet that goal within your parameters

VULNERABILITY SCAN

- Exhaustive catalog of possible issues
- Ranked by criticality
- Manually reviewed if you are lucky

You know what, just go read @DanielMiessler *"The Difference Between a Vulnerability Assessment and a Penetration Test"*

Get your priorities straight!

- Do you know what software is installed on your systems?
- Do you know what versions of software they are?
- Are those software installations patched?

If you are answering no, you probably need to do a Vulnerability Scan.

Does that Mean I shouldn't be talking about a pentest?

Probably

I mean seriously, you have way too much work to be doing.

But let's do it anyway, and here's why…

NOTHING SAYS YOU NEED TO LET ME UPGRADE THAT DEVICE LIKE THE PHRASE:

"We got to your SSN from the Internet because… "

So why this DIY pentest?

Shouldn’t we just get a firm to come do this for us?

So external tests are bad?

Let the battle begin!

Pushback

- It's just too expensive to hire a firm to do a pentest.
- It's still going to cost money, and time we don't have
- We've got all of these projects that we never get to work on, and this is just one more.

Response

- I agree, we can do it ourselves much cheaper.
- Not as much as you think, I saw a presentation where we can do it by repurposing a couple of old laptops and under a week of effort.
- This is a small one, that gets us the data we need to know which others should be priorities.

Gather your team!

Pirates Vs Ninjas

Both have benefits, today we are talking pirates.

Check out Kirk Hayes' *"Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues'*

Image Attribution: Sarah Thomas

Yeah, yeah, I get it. Pentests are good.

Get On With It!

One quick thing…

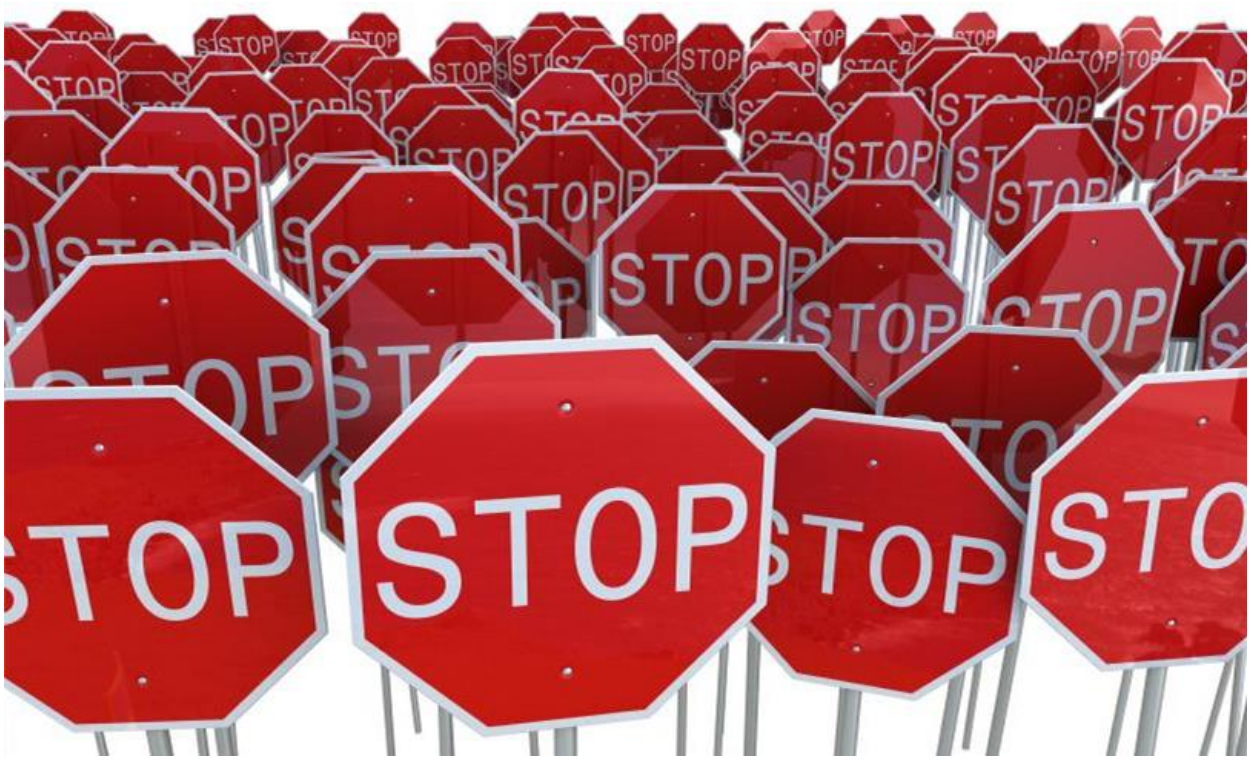
There are several standards for pentests available online.

- The Penetration Testing Execution Standard,
- ISECOM's Open Source Security Testing Methodology Manual,
- Even NIST has a version, but most of these are a little dated.

Review them, have a look and decide if they are right for you. Do some homework online.

Basic Assumptions

- You have permission to work on this “In your spare time”
- Minimal Hardware Purchase
- No Software Purchase
- You can download the stuff you need to do this on your normal work computer



You have permission to work on this in your spare time…

Is that in writing?

https://www.owasp.org/index.php/Authorization_form

Scoping and Goals

What are we going to test, and how do we know if it was successful?

Golden Tickets

These are your “Game Over” items.

Some examples are:

- Key personnel login credentials with successful login.
- Laying hands on the contents of a key sensitive database.
- Root / Local Admin / Domain Admin access
- Credit Card Data
- Stolen Laptop with data extraction
- Health Records

Shopping list

- Hak5 – Hakshop
  - 1 – BashBunny - $99
  - 1 – Rubber Ducky - $45
- Other source
  - 2 – Raspberry Pi with sd card /cases / power – $50
  - 1 - High gain wifi USB adapter - $30

All in, should be under $300

Building out your schedule

Week 1

- Approximately one week worth of time spent across the month before the test
- Build scope, write plan, GET PERMISSION, setup tools

Week 2

- Pentest week – Stake out a conference room and hide for the week
- Actively Testing

Week 3

- You will forget what you learned if you don't immediately write it down
- Take a full day or two to properly document the test results

Getting a foothold

- Physical
- Ducky
- Dropboxes
- Assumed compromise
- Others

Responder

Silently collect creds

Crack Hashes

- Responder will get hashed credentials, need to crack them

Password spraying

- Works AMAZING, can be done anywhere once you have the first creds

Command and Control setup

- Dropbox with PentestPi over Kali
- Or C&C using CobaltStrike/CoreImpact/Metasploit

Become Administrator

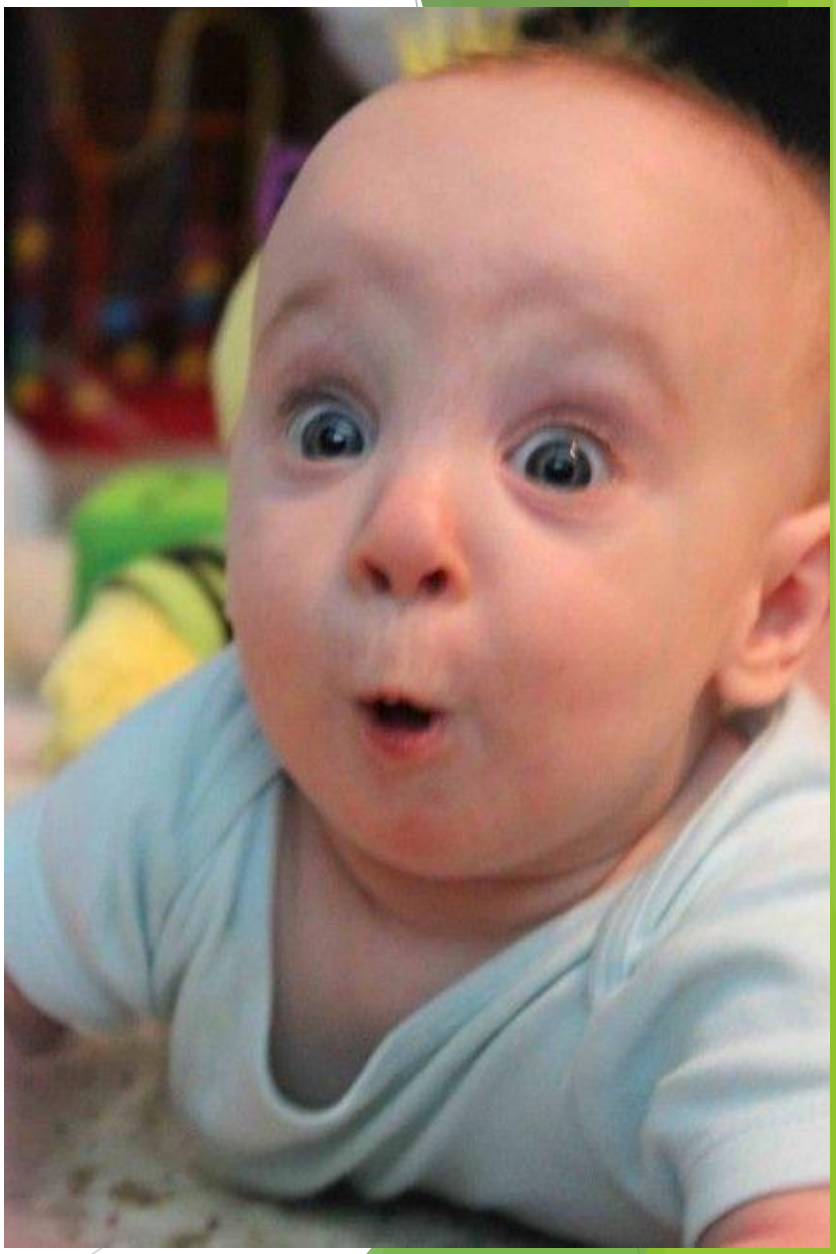
- Shared User/Admin Passwords
- Privilege Escalation Attacks
  - PowerUp

Exploitation and Lateral Movement

- At this point we root around shared drives as legit user
- Login to internal apps and servers
- Steal more Passwords with Mimikatz
  - This has worked for ZZ accounts as well

Surprises

- Physical is easy
- Password incrementing
- Password reuse
- Mimikatz patch installed but not enabled



Rule 31

After the test, choose 3 findings that can be fixed.

- The most critical issue
- The easiest non-trivial issue to fix
- The most visible issue

Conclusion

- It’s way easier than you think it is
- Just do one to see for yourself and your agency
  - Annually if you can swing it
- Gets some great buy-in because execs can see results
- Implement your pentester’s recommendations to make it harder for them next year
- Simplest controls make the most impact

Mitigations

- Disable LLMNR, NetBIOS over TCP, WPAD
- Remove Local Admin Rights from users
- Different local admin passwords or disable network use of local accounts
- Two factor for server access
- Mitigate mimikatz with this: https://www.praetorian.com/blog/mitigating-mimikatz-wdigest-cleartext-credential-theft
- Private VLANS

Questions

@andrew_hallberg
@grandomthoughts

Upcoming Events

Security Audits of IT Systems

- According to SEC 502, all IT security audits must follow either:
  - GGAS (Generally Accepted Government Auditing Standard) Yellow Book
  - IIAS (Institute of Internal Auditors Standards) Red Book
  - AICPA (American Institute of Certified Public Accountants)
- This includes all internal audits and all contracted audits

Reporting IT Security Audit Results to VITA

- The official audit report must include an attestation as to the audit standard used.
- This includes internal audits and audits performed by external organizations.
- Reports without this statement of assurance to meet the SEC-502 standard may be rejected.

Future ISOAG

August 30 ,2017 1:00 - 4:00 pm @ CESC

Speakers: Eddie McAndrew, Impact Makers

Barry Davis,DSS

Benjamin Sady Dixon Hughes Goodman

ISOAG meets the 1st Wednesday of each month in 2017

Virginia Information Technologies Agency

Announcement: VASCAN Conference 2017

Virginia Alliance for Secure Computing & Networking
VASCAN

IOT: The S Stands for Security

Date: September 28-29
Location: Virginia Tech, Blacksburg VA

Keynote Speaker:
Doug Wylie
Director Industrials &
Infrastructure Portfolio
SANS Institute

To Register: http://www.cpe.vt.edu/vascan/

OSIG Training

Planning and Assessing Access Controls in Today's IT Environment

Instructor: David Cole – SysAudits.com

Date: October 31, 2017

Location: Virginia Credit Union Operations Center / 1st Floor Training Conference Room

Address: 7500 Boulder View Dr.
North Chesterfield, VA 23225

Pricing Terms: $175.00 **REGISTRATION LINK:**

https://osig.virginiainteractive.org

CPE: 8 hours

General Overview:

This course will provide an overview of access controls that are commonly being used in today's complex environments. Walk through of two-factor deployments, application web-proxies, DMZ environments and designs; and cloud application hosting. In addition, an overview of vulnerability management program and walk through of key audit areas.

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk